

UCCE\PCCE — 在2008伺服器上獲取和上傳 Windows Server 自簽名證書或證書頒發機構 (CA)證書的過程

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[步驟 1.從Internet資訊服務\(IIS\)管理器生成CSR](#)

[步驟 2.將CA簽名的證書上傳到Internet Information Services\(IIS\)管理器](#)

[步驟 3.將簽名的CA證書繫結到預設網站](#)

[驗證](#)

[疑難排解](#)

[相關思科支援社群討論](#)

簡介

本文描述如何在Unified Contact Center Enterprise(UCCE)Windows 2008 R2伺服器上配置自簽名證書或證書頒發機構(CA)證書。

必要條件

需求

思科建議您瞭解簽名和自簽名證書流程。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Windows 2008 R2
- UCCE 10.5(1)

設定

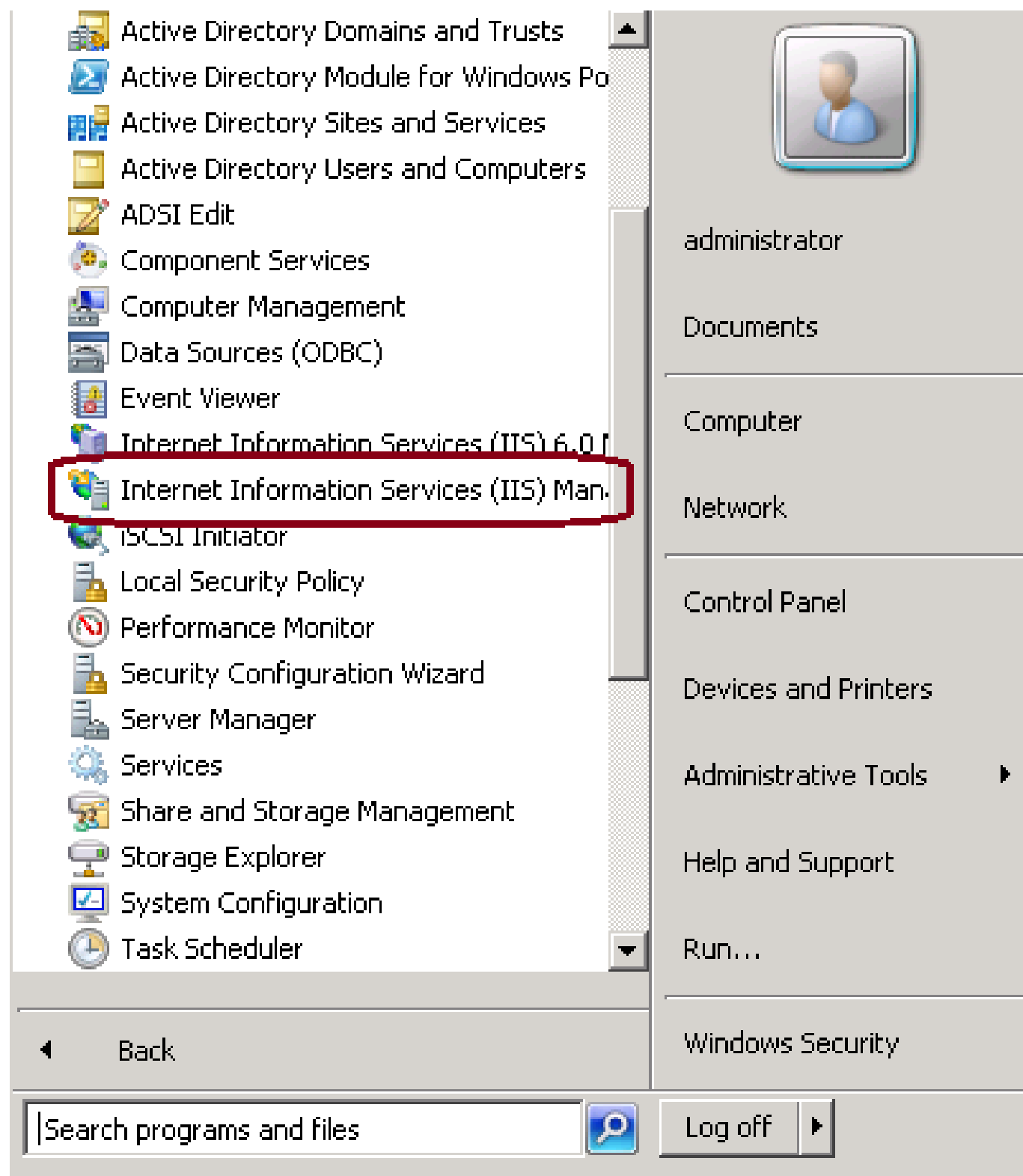
在Windows伺服器上為HTTPS通訊設定證書是一個三步過程

- 從Internet資訊服務(IIS)管理器生成證書簽名請求(CSR)

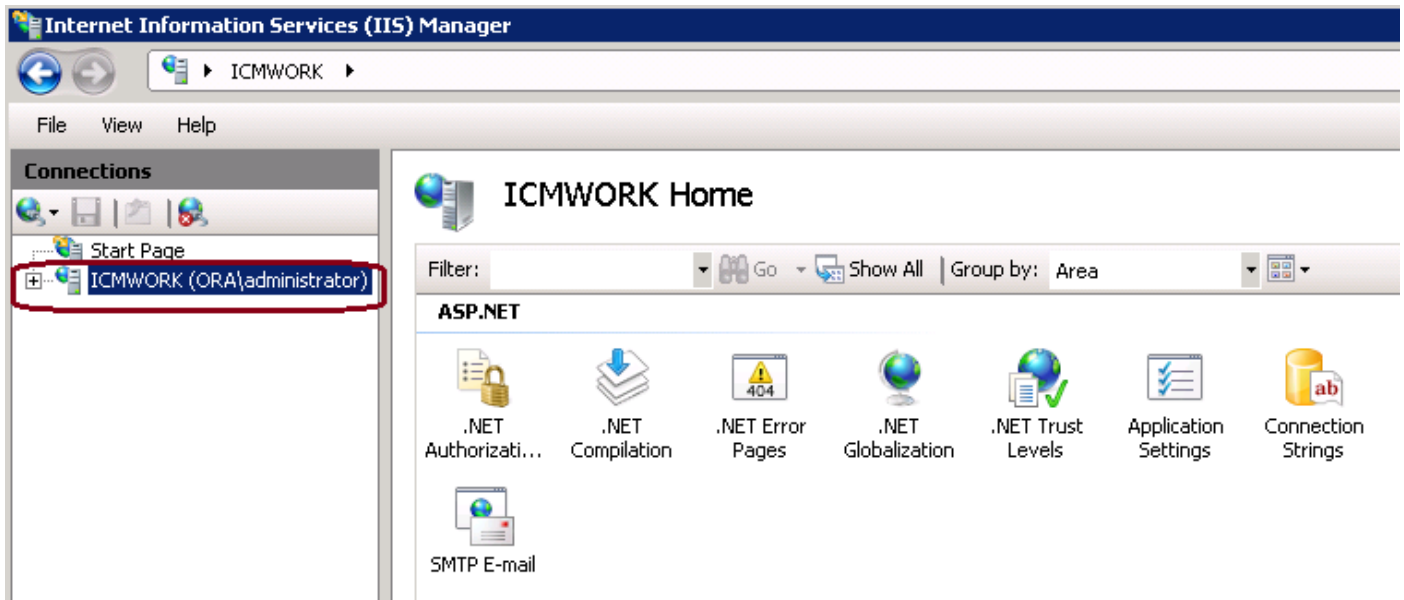
- 將CA簽名的證書上傳到Internet Information Services(IIS)管理器
- 將簽名的CA證書繫結到預設網站

步驟 1.從Internet資訊服務(IIS)管理器生成CSR

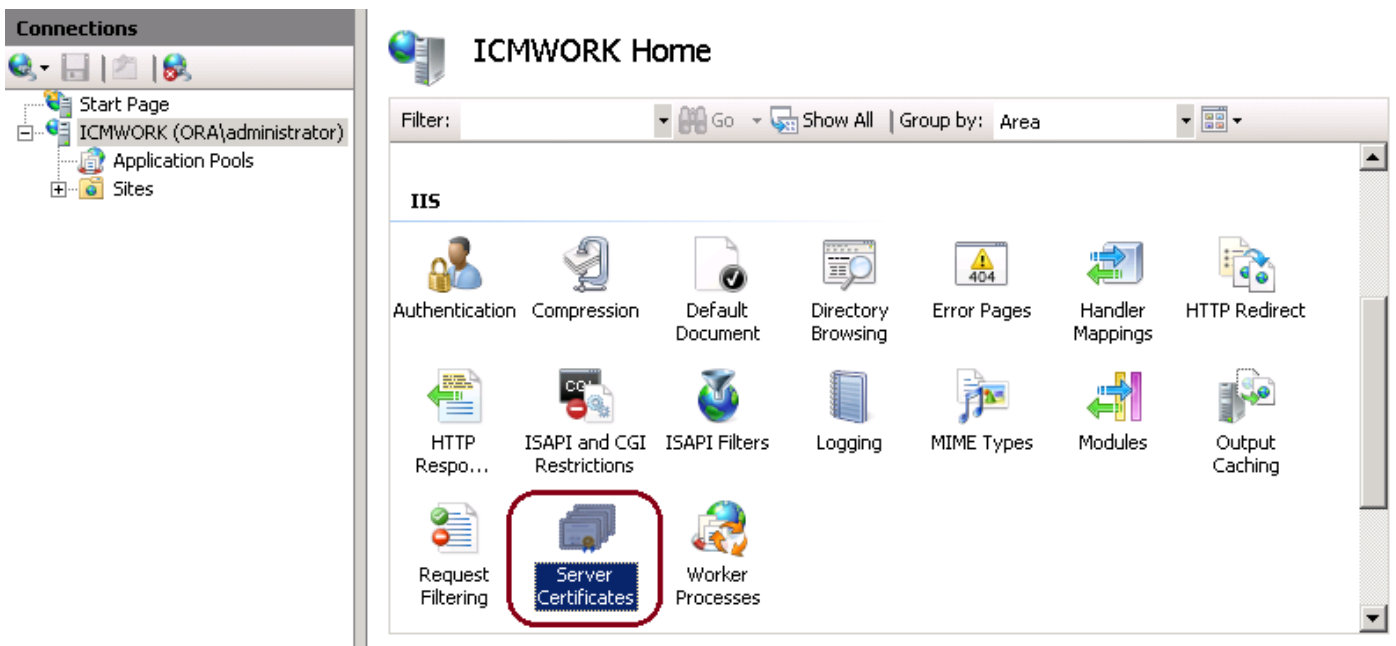
1.登入到Windows，按一下「開始」>「運行」>「所有程式」>「管理工具」>「Internet Information Services(IIS)管理器」，如下圖所示。如果存在IIS版本6，則不要選擇它。



2.在左側的「連線」窗格中，選擇伺服器名稱，如下圖所示。



3. 在中間視窗窗格中，選擇 IIS > Server Certificates。按兩下 Server Certificates 以生成證書視窗，如下圖所示。



4. 在右窗格中，按一下 Actions > Create Certificate Request，如下圖所示。

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

Create Self-Signed Certificate...




Help

Online Help

5.要完成證書請求，請輸入「公用名」、「組織」、「組織單位」、「城市/地區」、「州/省」和「國家/地區」，如下圖所示。

Request Certificate ? X

 **Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

City/locality:


State/province:

Country/region:

Previous Next Finish Cancel

6.按一下「下一步」修改加密和安全位長度，建議至少使用2048以提高安全性，如下圖所示。

Request Certificate ? X

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

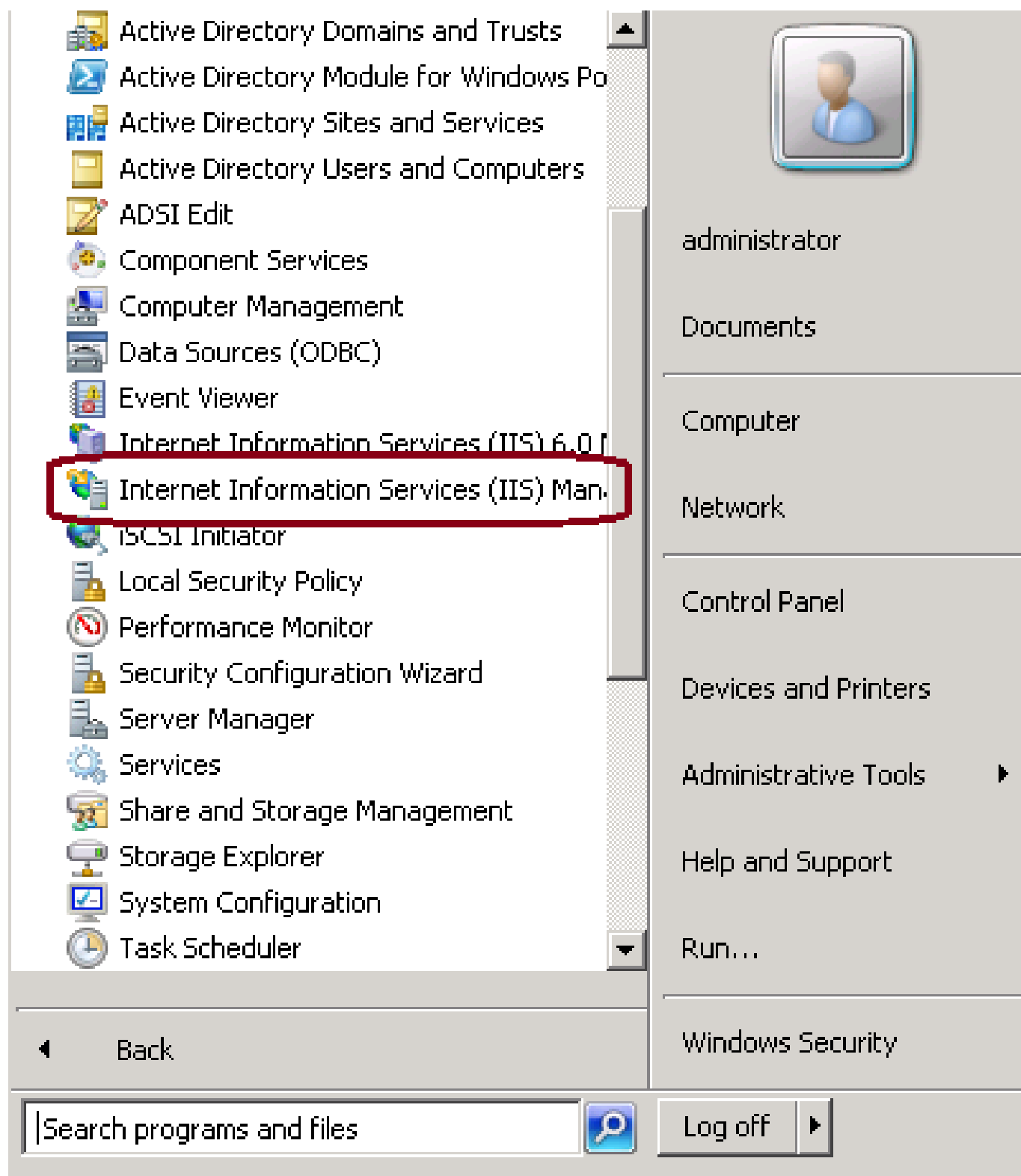
Bit length:

7.將證書請求儲存在所需的位置，該位置將儲存為.TXT格式，如下圖所示。

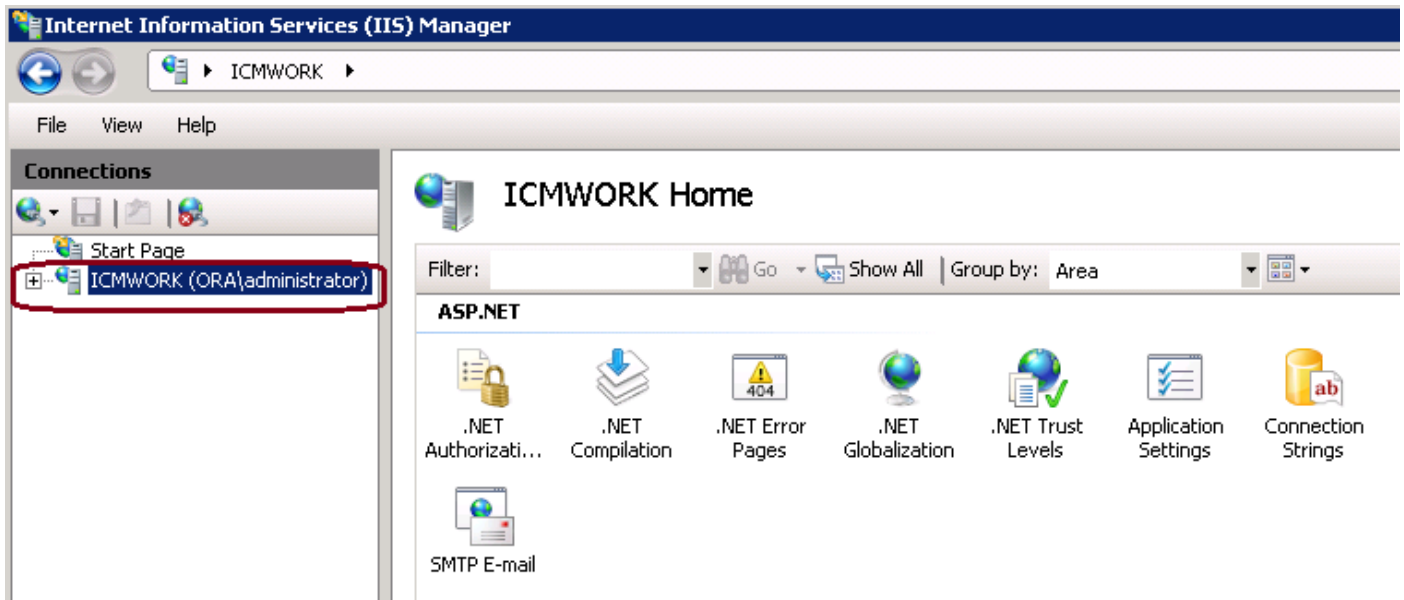
8.提供此檔案供管理內部CA或外部CA服務請求的團隊簽署，如下圖所示。

步驟 2.將CA簽名的證書上傳到Internet Information Services(IIS)管理器

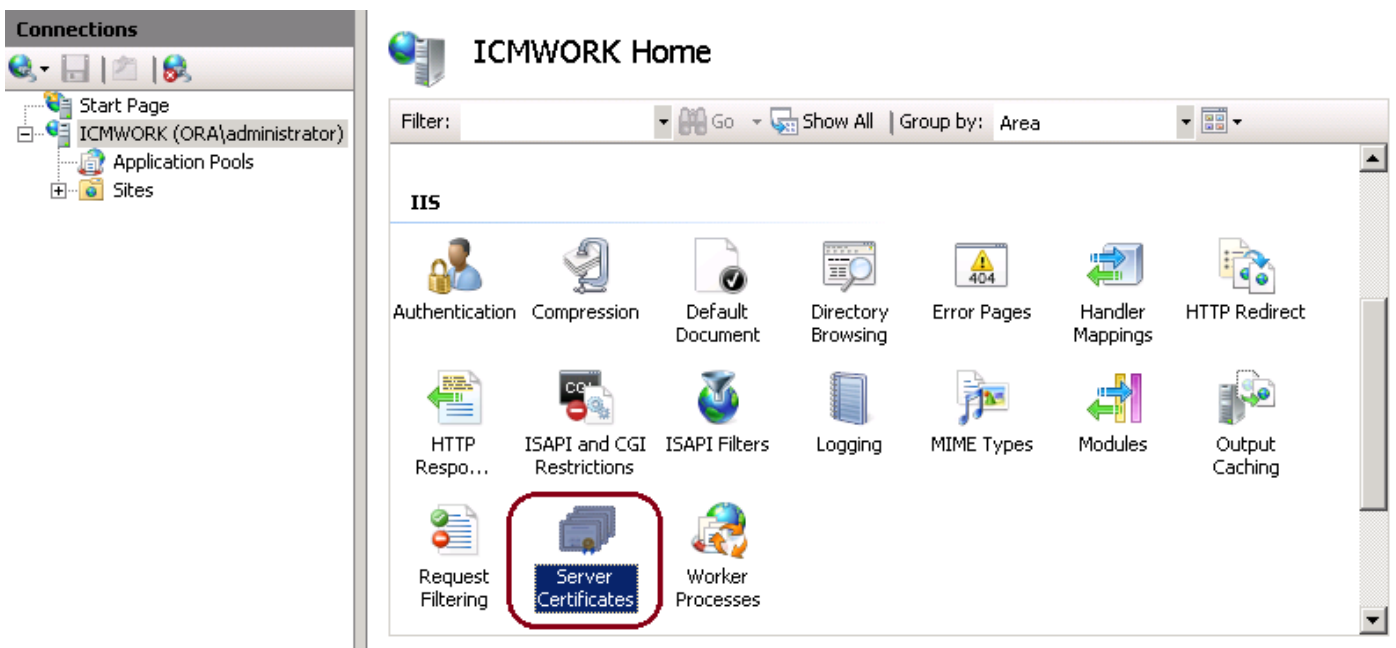
1.登入到Windows，按一下「開始」>「運行」>「所有程式」>「管理工具」>「Internet Information Services(IIS)管理器」，如下圖所示。如果存在IIS版本6，則不要選擇它。



2.在左側的「連線」窗格中，選擇伺服器名稱，如下圖所示。



3. 在中間視窗窗格中，選擇 IIS > Server Certificates。按兩下 Server Certificates 以生成證書視窗，如下圖所示。



4. 在右窗格中，按一下 Actions > Complete Certificate Request，如下圖所示。

Actions

Import...

Create Certificate Request...

Complete Certificate Request...

Create Domain Certificate...

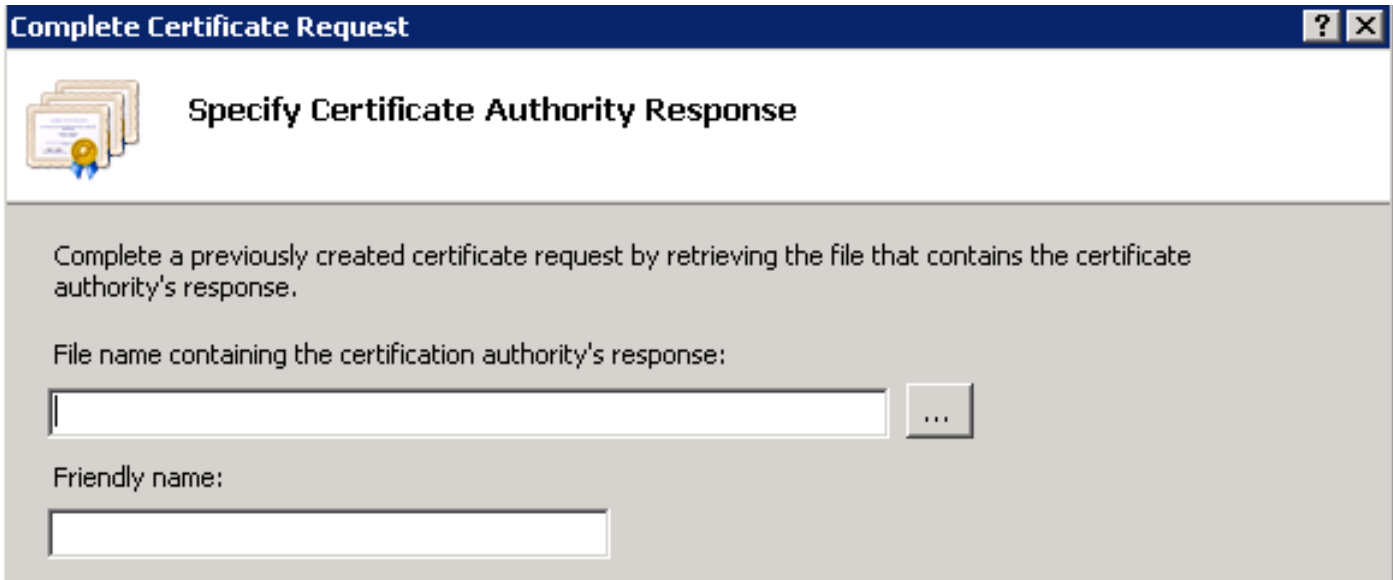
Create Self-Signed Certificate...



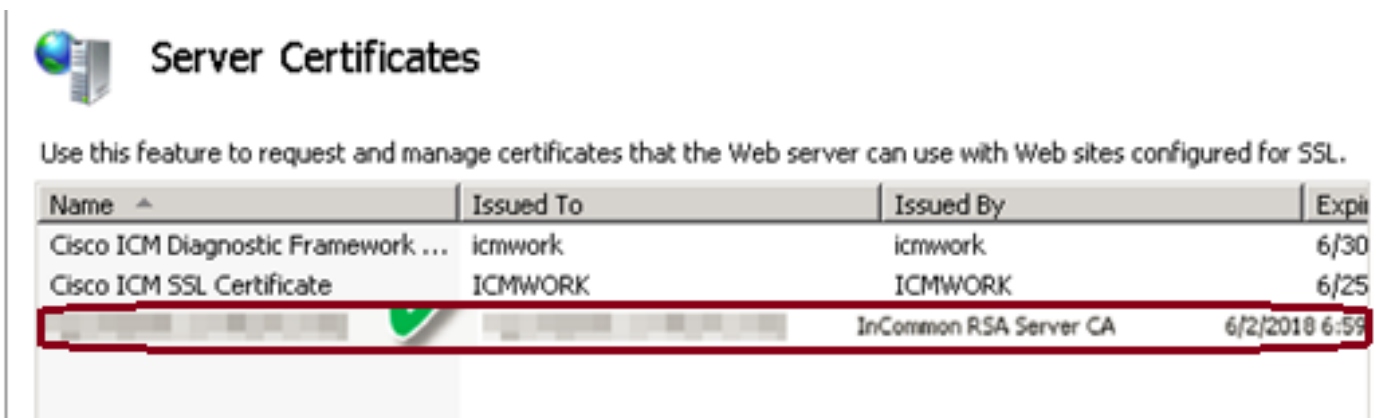
Help

Online Help

5.在此步驟之前，請確保已簽名的證書採用.CER格式並已上傳到本地伺服器。按一下.....按鈕瀏覽.CER檔案。在友好名稱內，使用伺服器的FQDN，如下圖所示。

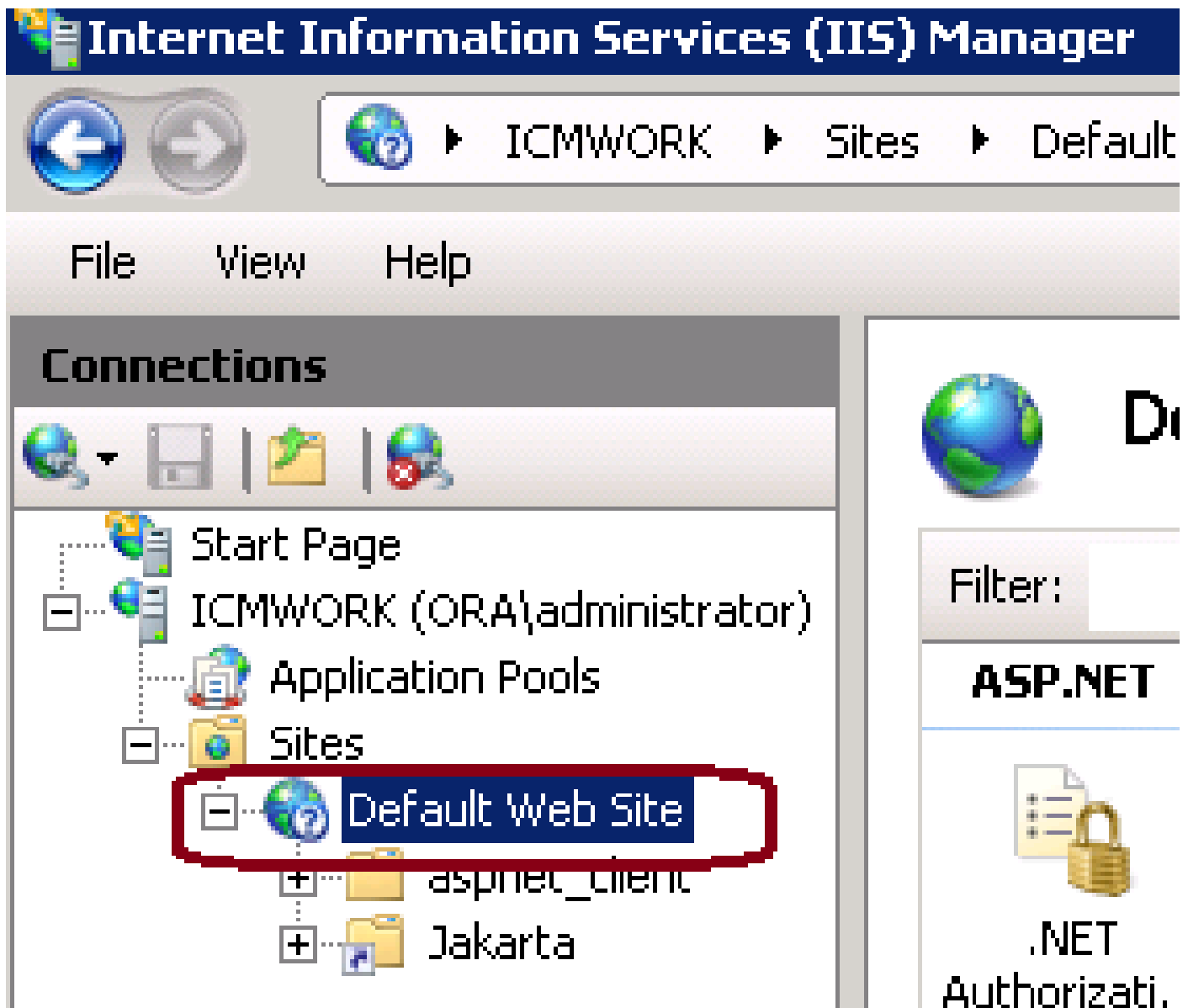


6.按一下「OK」以上傳憑證。完成後，確認證書現在顯示在「伺服器證書」視窗中，如下圖所示。



步驟 3.將簽名的CA證書繫結到預設網站

1.在IIS管理器的「連線」視窗平面下，按一下左邊的<server_name> > 「站點」 > 「預設網站」，如下圖所示。



2.在右側的「操作」視窗窗格中，按一下「繫結」，如下圖所示。

Actions



Explore

Edit Permissions...

Edit Site

Bindings...

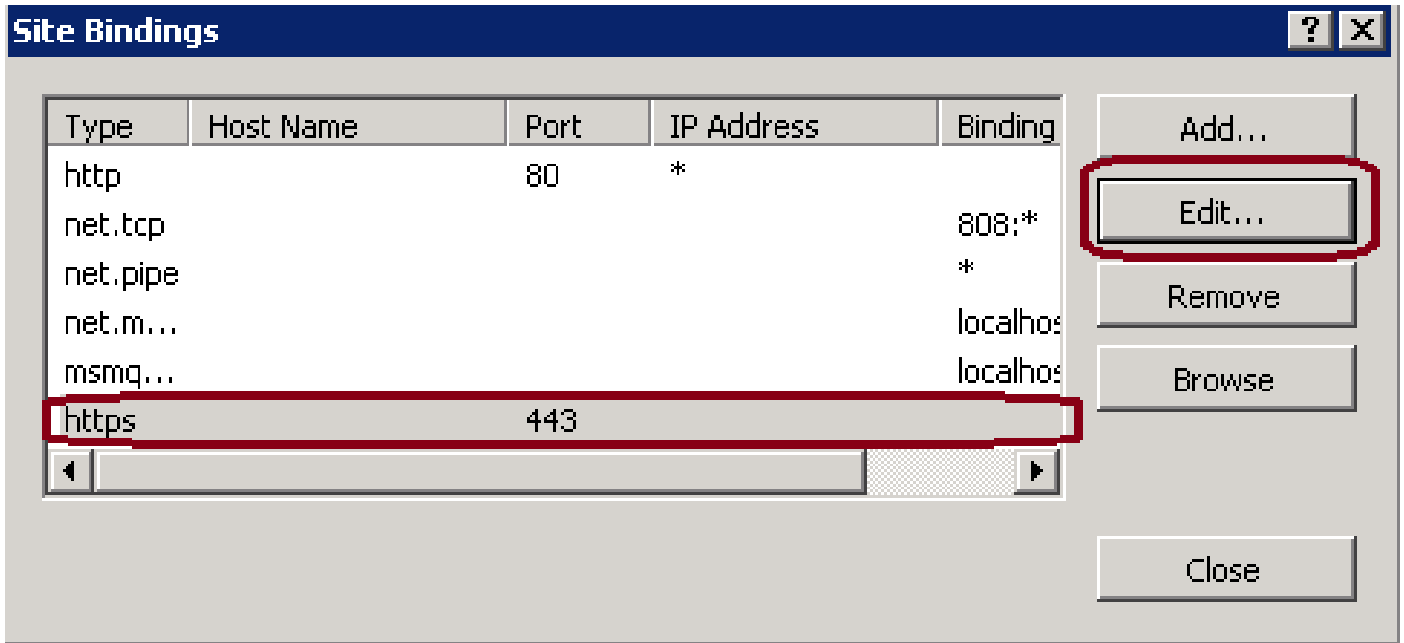


Basic Settings...

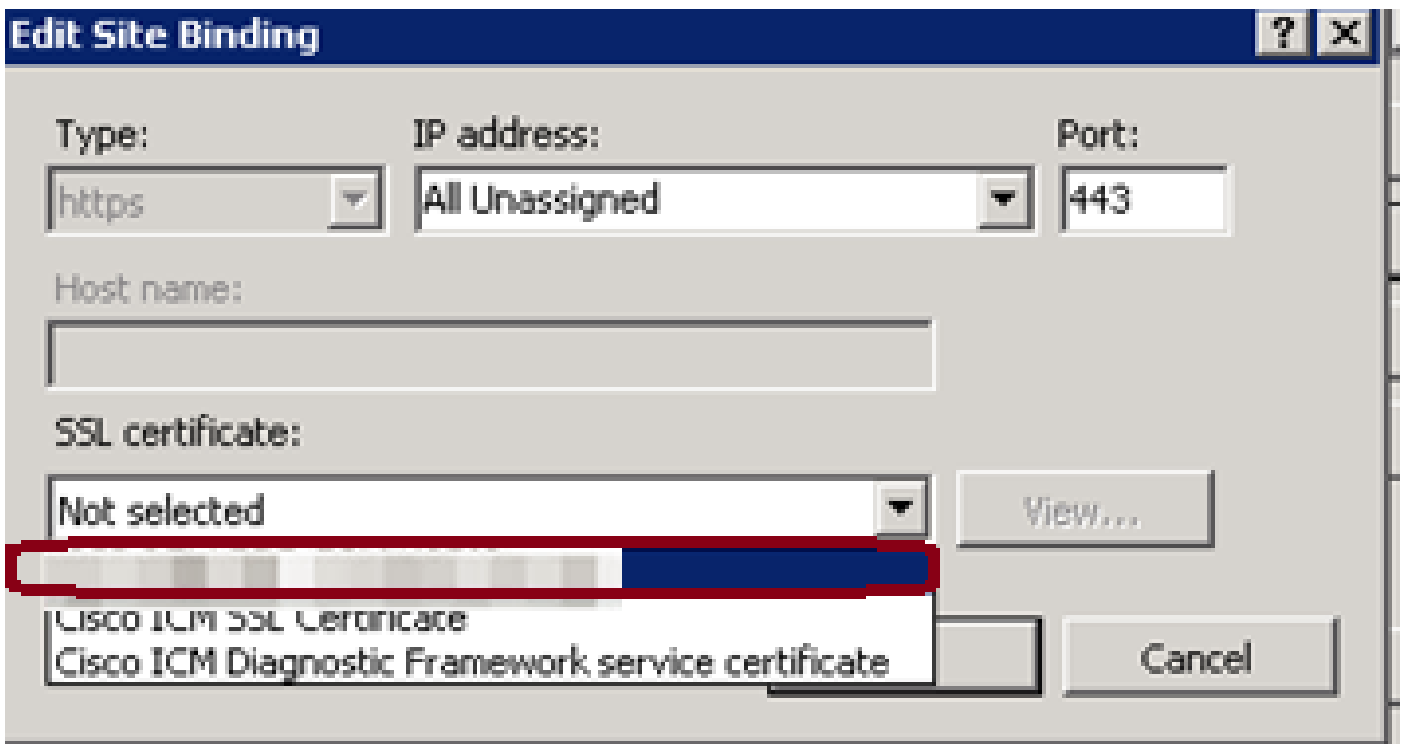
View Applications

View Virtual Directories

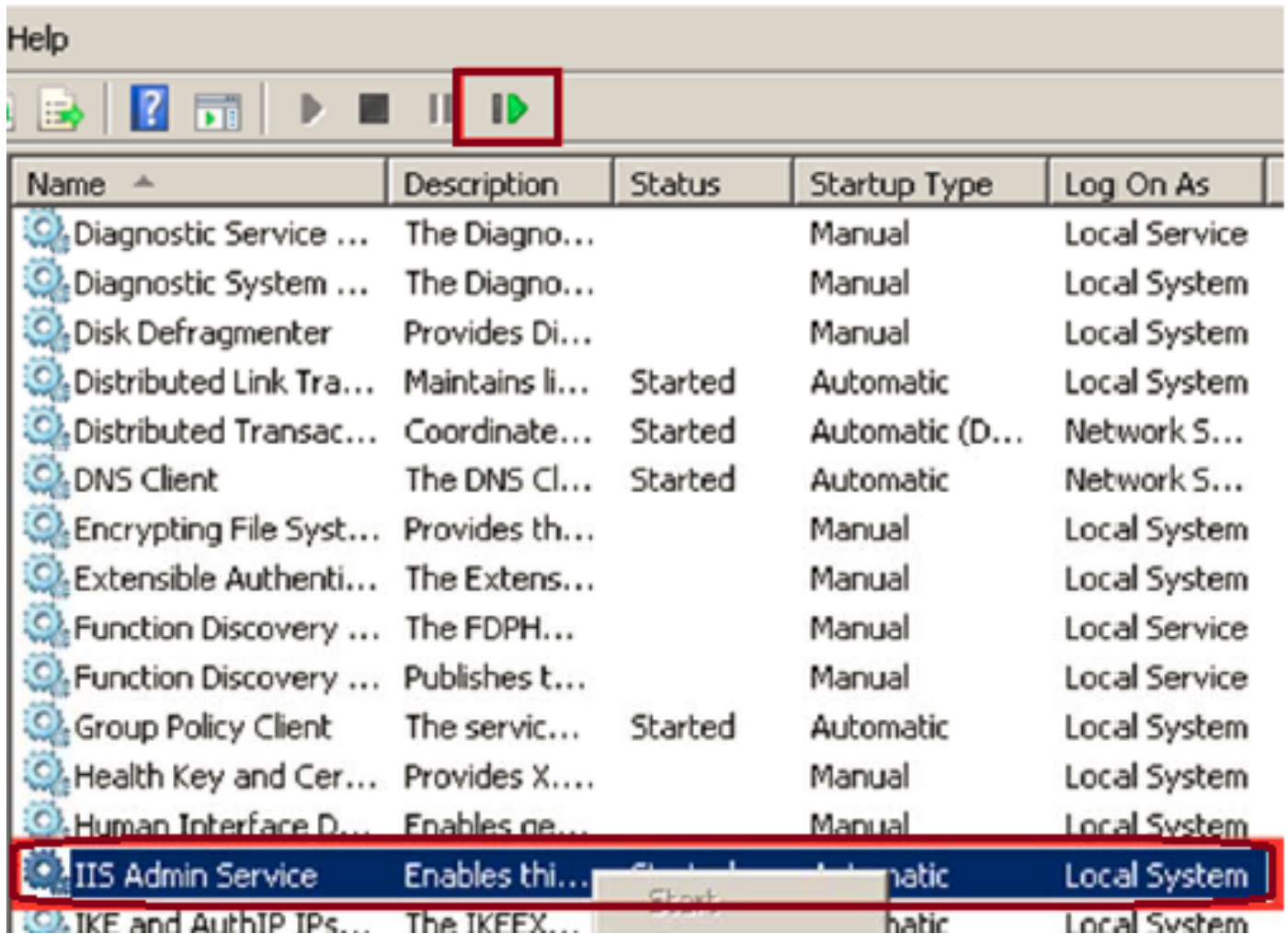
3.在「站點繫結」視窗中，按一下https以突出顯示更多選項。按一下「Edit」以繼續，如下圖所示。



4.在SSL證書引數下，按一下向下箭頭以選擇以前上傳的簽名證書。檢視簽名證書以驗證證書路徑和值是否與本地伺服器匹配。完成後，請按「確定」，然後按「關閉」退出「站點繫結」視窗，如下圖所示。



5.按一下開始>運行> services.msc，在Services MMC管理單元下重新啟動IIS管理服務，如下圖所示。



6.如果成功，客戶端Web瀏覽器在輸入網站的FQDN URL時不應提示任何證書錯誤警告。

注意：如果IIS管理服務丟失，請重新啟動全球資訊網發佈服務。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。